Training and Evaluation Outline Report

Task Number: 71-8-5900

Task Title: Conduct Cyber/Electromagnetic Activities (Battalion - Corps)

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	ADP 3-0	Unified Land Operations	Yes	No
	FM 3-13	INFORMATION OPERATIONS: DOCTRINE, TACTICS, TECHNIQUES, AND PROCEDURES	Yes	Yes
	FM 5-0	THE OPERATIONS PROCESS	Yes	No
	FM 6-0	MISSION COMMAND	Yes	No
	JOINT PUB 3-13.1	Electronic Warfare	Yes	No

Condition: The command has received an operations plan, or warning, operations, or fragmentary order from higher headquarters and is exercising mission command. The commander has issued guidance on conducting cyber-electromagnetic activities. The command has established communications with subordinate and adjacent units, and higher headquarters. The mission commandsystem is operational and processing information in accordance with standard operating procedures. This task can be performed in hours of daylight or limited visibility in various environment conditions. The unit has received guidance on the rules of engagement. Some iterations of this task should be performed in MOPP.

Standard: The staff led by the G6 section supports the Commander's intent and guidance by conducting cyber/electromagnetic activities in order to seize, retain, and exploit advantages over adversaries and enemies in both cyberspace and across the electromagnetic spectrum, denying and degrading adversary and enemy use of the same and protecting friendly mission command networks, thereby enabling the overall operation. Note: Task steps and performance measures may not apply to every unit or echelon. Prior to evaluation, coordination should be made between evaluator and the evaluated units' higher headquarters to determine the performance measures that may not be evaluated.

Note 1: Coordinate with the Staff Judge Advocate to ensure compliance with the status of forces agreement, rules of engagement and international law. Cyber/electromagnetic activities are divided into two lines of effort: The cyberspace operations line of effort and the electronic warfare line of effort. These lines of effort may rely on the same capabilities and enablers to accomplish these effects and must be synchronized and integrated closely to ensure unity of effort in words, images, and actions. The components of the cyberspace operations line of effort integrate with the components of the electronic warfare line of effort and electromagnetic spectrum operations.

Note 2: Task steps and performance measures may not apply to every staff, unit or echelon. Prior to evaluation, coordination should be made between evaluator and the evaluated staffs or units' higher headquarters to determine the performance measures that may not be evaluated.

Special Equipment: None

Safety Level: Low

Task Statements

Cue: None

DANGER

Leaders have an inherent responsibility to conduct Composite Risk Management to ensure the safety of all Soldiers and promote mission accomplishment.

WARNING

Composite Risk Management is the Army's primary decision-making process to identify hazards, reduce risk, and prevent both accidental and tactical loss. All soldiers have the responsibility to learn and understand the risks associated with this task.

CAUTION

Identifying hazards and controlling risks across the full spectrum of Army functions, operations, and activities is the responsibility of all Soldiers.

Remarks: Task content last updated: 30 Jan 2012.

Notes: None

TASK STEPS

1. The staff, led by the G6/S6 section, synchronizes and integrates cyber/electromagnetic activities by integrating the component of cyberspace line of effort with the components of electronic warfare line of effort and electromagnetic spectrum operations.

2. The staff, led by the G6/S6 section, coordinates and employs the cyberspace operations line of effort to accomplish the objective in and through cyberspace:

a. Cyber situational awareness; continuously provides updates to activities in and through cyberspace and the electromagnetic spectrum:

(1) Assess threat cyber capabilities and intentions.

(2) Assess friendly and threat cyber vulnerabilities.

(3) Monitor, protect, and prioritize networks.

(4) Assess the operational impact of network disruptions.

(5) Respond to network outages or attacks.

(6) Dynamically reallocate network traffic.

b. Conduct network operations that include activities to defend the global information grid.

c. Conduct cyber warfare; targeting computer and telecommunications networks, embedded processors and controllers in equipment, systems, and infrastructure to better:

(1) Study and characterize the cyber threat.

(2) Detect, identify and characterize enemies.

(3) Contribute to cyber situational awareness.

(4) Conduct cyber exploitation, attack and defense.

(5) Assists attack investigations to determine attribution.

(6) Deny, disrupt and destroy enemies.

3. The staff, led by the G6/S6 section, synchronizes and integrates the electronic warfare line of effort to control the electromagnetic spectrum and/or attack the threat through:

a. Offensive or defensive electronic attack that employ electromagnetic energy, directed energy or antiradiation weapons to attack facilities or equipment with the intent of degrading, or destroying threat combat power.

b. Employ electronic protection measures:

(1) Protect from threat attack.

(2) Protect from accidental friendly attack.

(3) Deny the threat the use of the electromagnetic spectrum to guide or trigger weapons.

(4) Verify the protection of friendly capabilities:

(a) Brief force personnel on the electronic warfare threat.

(b) Safeguard electronic system capabilities during exercises and training.

(c) Coordinate and deconflict electromagnetic spectrum usage.

(d) Train on electronic protection active and passive measures.

(e) Minimize the vulnerability of friendly receivers to threat jamming.

c. Verify electronic support systems are in place to produce information or intelligence to:

(1) Corroborate other sources of information or intelligence.

(2) Conduct or direct electronic attack operations.

(3) Initiate self-protection measures.

(4) Task weapon systems.

(5) Support electronic protection efforts.

(6) Create or update electronic warfare databases.

(7) Support information activities.

4. The staff, led by the G6/S6 section, plans and manages the following electromagnetic spectrum operations:

a. Electronic attack.

b. Electronic protect.

c. Electronic support.

d. Communication networks.

e. Information assurance.

f. Identification friend or foe.

g. Unmanned ground systems.

h. Unarmed aircraft systems.

i. Information dissemination management.

j. Electronic warfare operations.

k. Host coordination.

l. Frequency assignments.

m. Network management.

n. Policy.

(Asterisks indicates a leader performance step.)

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. The staff, led by the G6/S6 section, synchronized and integrated cyber/electromagnetic activities by integrating the component of cyberspace line of effort with the components of electronic warfare line of effort and electromagnetic spectrum operations.			
2. The staff, led by the G6/S6 section, coordinated and employed the cyberspace operations line of effort to accomplish the objective in and through cyberspace:			
a. Cyber situational awareness; continuously provided updates to activities in and through cyberspace and the electromagnetic spectrum:			
(1) Assessed threat cyber capabilities and intentions.			
(2) Assessed friendly and threat cyber vulnerabilities.			
(3) Monitored, protected, and prioritized networks.			
(4) Assessed the operational impact of network disruptions.			
(5) Responded to network outages or attacks.			
(6) Dynamically reallocated network traffic.			
b. Conducted network operations that include activities to defend the global information grid.			
c. Conducted cyber warfare; targeted computer and telecommunications networks, embedded processors and controllers in equipment, systems, and infrastructure to better:			
(1) Studied and characterized the cyber threat.			
(2) Detected, identified and characterized enemies.			
(3) Contributed to cyber situational awareness.			
(4) Conducted cyber exploitation, attack and defense.			
(5) Assisted attack investigations to determine attribution.			
(6) Denied, disrupted and destroyed enemies.			
3. The staff, led by the G6/S6 section, synchronized and integrated the electronic warfare line of effort to control the electromagnetic spectrum and/or attack the threat through:			
a. Offensive or defensive electronic attack that employed electromagnetic energy, directed energy or antiradiation weapons to attack facilities or equipment with the intent of degrading, or destroying threat combat power.			
b. Employed electronic protection measures:			
(1) Protected from threat attack.			
(2) Protected from accidental friendly attack.			
(3) Denied the threat the use of the electromagnetic spectrum to guide or trigger weapons.			
(4) Verified the protection of friendly capabilities:			
(a) Briefed force personnel on the electronic warfare threat.			
(b) Safeguarded electronic system capabilities during exercises and training.			
(c) Coordinated and deconflict electromagnetic spectrum usage.			
(d) Trained on electronic protection active and passive measures.			
(e) Minimized the vulnerability of friendly receivers to threat jamming.			
c. Verified electronic support systems are in place to produce information or intelligence to:			
(1) Corroborated other sources of information or intelligence.			
(2) Conducted or directed electronic attack operations.			
(3) Initiated self-protection measures.			
(4) Tasked weapon systems.			
(5) Supported electronic protection efforts.			
(6) Created or updated electronic warfare databases.			
(7) Supported information activities.			
4. The staff, led by the G6/S6 section, planned and managed the following electromagnetic spectrum operations:			
a. Electronic attack.			

b. Electronic protect.			
c. Electronic support.			
d. Communication networks.			
e. Information assurance.			
f. Identification friend or foe.			
g. Unmanned ground systems.			
h. Unarmed aircraft systems.			
i. Information dissemination management.			
j. Electronic warfare operations.			
k. Host coordination.			
l. Frequency assignments.			
m. Network management.			
n. Policy.			

TASK PERFORMANCE / EVALUATION SUMMARY BLOCK							
ITERATION	1	2	3	4	5	M	TOTAL
TOTAL PERFORMANCE MEASURES EVALUATED							
TOTAL PERFORMANCE MEASURES GO							
TRAINING STATUS GO/NO-GO							

ITERATION: **1 2 3 4 5 M**

COMMANDER/LEADER ASSESSMENT: **T P U**

Mission(s) supported: None

MOPP: Sometimes

MOPP Statement: None

NVG: Never

NVG Statement: None

Prerequisite Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-8-3502	Assess Electronic Warfare Operations (Division - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-5110	Plan Operations Using the Military Decision Making Process (Battalion - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Collective Task(s):

Step Number	Task Number	Title	Proponent	Status
	71-8-3501	Coordinate Electronic Warfare (Division - Corps)	71 - Combined Arms (Collective)	Approved
	71-8-3510	Conduct Electronic Attack (Division - Corps)	71 - Combined Arms (Collective)	Approved

Supporting Individual Task(s):

Step Number	Task Number	Title	Proponent	Status
	011-420-0031	Implement Operations in an Electronic Warfare Environment	011 - Aviation (Individual)	Approved
	093-948-B120	Supervise Maintenance of Computer Networks and Associated Equipment	093 - Munitions and Electronics Maintenance (Individual)	Approved
	113-322-7008	Plan Situational Awareness (SA) Services over a TCP/IP Network	113 - Signal (Individual)	Approved
	113-337-7002	Establish Global Information Grid (GIG) Circuit Switched Network Services within an Enterprise Network	113 - Signal (Individual)	Approved
	113-367-5001	Implement Network Protection Measures	113 - Signal (Individual)	Approved
	113-473-4008	Plan a Secure Network Architecture	113 - Signal (Individual)	Approved
	113-616-2018	Conduct Electronic Counter-Countermeasures (ECCM) Network Controller (ENC) Operations within the Defense Satellite Communications System (DSCS)	113 - Signal (Individual)	Approved
	113-642-6002	Plan for Electronic Warfare (EW) Measures	113 - Signal (Individual)	Approved
	150-029-2004	Identify Electronic Warfare (EW) Capabilities in Full Spectrum Operations	150 - Combined Arms (Individual)	Approved
	150-029-5001	Report Electromagnetic Spectrum Interference	150 - Combined Arms (Individual)	Approved
	150-718-5111	Participate in the Military Decision Making Process	150 - Combined Arms (Individual)	Approved
	301-52N-6817	Direct Synchronization of Signals Intelligence (SIGINT) and Electronic Warfare (EW) Interoperability	301 - Intelligence (Individual)	Approved
	441-041-2038	Perform Electronic Counter-Countermeasures (ECCM) Operations	441 - Air Defense (Individual)	Approved

Supporting Drill Task(s): None

TADSS

Step ID	TADSS ID	Title	Product Type	Quantity
No TADSS specified				

Equipment (LIN)

Step ID	LIN	Nomenclature	Qty
No equipment specified			

Materiel Items (NSN)

Step ID	NSN	LIN	Title	Qty
No equipment specified				

Environment: Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT.

Safety: In a training environment, leaders must perform a risk assessment in accordance with FM 5-19, Composite Risk Management. Leaders will complete a DA Form 7566 COMPOSITE RISK MANAGEMENT WORKSHEET during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, NBC Protection, FM 3-11.5, CBRN Decontamination. .